

CLAIMS

What is claimed is:

1. A method comprising:
identifying data to be signed;
establishing parameter data for use with signature generating logic that encrypts data based on a Jacobian of a curve, said Jacobian having a genus exceeding one, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve;
determining private key data and corresponding public key data using said signature generating logic; and
signing said identified data with said private key data using said signature generating logic to create a corresponding digital signature.

2. The method as recited in Claim 1, wherein said identified data includes a message $m \in \{0, 1\}^*$.

3. The method as recited in Claim 2, wherein said parameter data establishes a base group G and a generator g as system parameters for said signature generating logic.

4. The method as recited in Claim 3, wherein determining said private key data and said public key data includes:

picking $x \in \mathbb{Z}_p^*$; and

1 computing $v \leftarrow g^x$, wherein said public key data includes v and said private
2 key data includes x .

3
4 5. The method as recited in Claim 4, wherein signing said identified
5 data using with said private key data using said signature generating logic further
6 includes:

7 determining $h \leftarrow h(m)$, and $\sigma \leftarrow h^x$, using at least one hash function, said
8 private key data x and said message m , wherein said digital signature includes σ .

9
10 6. The method as recited in Claim 5, wherein said hash function
11 includes a full-domain hash function $h: \{0, 1\}^* \rightarrow G$.

12
13 7. The method as recited in Claim 5, wherein said hash function
14 includes a hash function $h': \{0, 1\}^* \rightarrow G \cup \{\perp\}$, that outputs an element of
15 G or \perp indicating a failure.

16
17 8. The method as recited in Claim 1, further comprising:
18 outputting said digital signature.

19
20 9. The method as recited in Claim 8, further comprising:
21 determining if said digital signature is valid using signature verifying logic.

22
23 10. The method as recited in Claim 9, wherein said signature verifying
24 logic is configured using said parameter data and said parameter data establishes a
25

1 base group G and a generator g as system parameters for said signature verifying
2 logic.

3
4 11. The method as recited in Claim 10, wherein:

5 said public key data includes public key data v ;

6 said identified data includes a message m ;

7 said digital signature includes signature σ ; and

8 determining if said digital signature is valid using said signature verifying
9 logic further includes:

10 determining $h \leftarrow h(m)$ using at least one hash function, and

11 verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple.

12
13 12. The method as recited in Claim 1, wherein said digital signature is
14 included in a product ID.

15
16 13. A computer-readable medium having computer implementable
17 instructions for causing at least one processing unit to perform acts comprising:

18 providing signature generating logic capable of digitally signing identified
19 data;

20 configuring said signature generating logic using parameter data, said
21 signature generating logic being configured to digitally sign said identified data
22 based on a Jacobian of a curve, said Jacobian having a genus greater than one, said
23 parameter data causing said signature generating logic to select at least one Gap
24 Diffie-Hellman (GDH) group of elements relating to said curve;

1 determining private key data and corresponding public key data using said
2 signature generating logic; and

3 signing said identified data with said private key data using said signature
4 generating logic to create a corresponding digital signature.

5
6 14. The computer-readable medium as recited in Claim 13, wherein said
7 identified data includes a message $m \in \{0, 1\}^*$.

8
9 15. The computer-readable medium as recited in Claim 14, wherein said
10 parameter data establishes a base group G and a generator g as system parameters
11 for said signature generating logic.

12
13 16. The computer-readable medium as recited in Claim 15, wherein
14 determining said private key data and said public key data includes:

15 picking $x \in \mathbb{Z}_p^*$; and

16 computing $v \leftarrow g^x$, wherein said public key data includes v and said private
17 key data includes x .

18
19 17. The computer-readable medium as recited in Claim 16, wherein
20 signing said identified data using with said private key data using said signature
21 generating logic further includes:

22 determining $h \leftarrow h(m)$, and $\sigma \leftarrow h^x$, using at least one hash function, said
23 private key data x and said message m , wherein said digital signature includes σ .

1 18. The computer-readable medium as recited in Claim 17, wherein said
2 hash function includes a full-domain hash function $h: \{0, 1\}^* \rightarrow G$.

3
4 19. The computer-readable medium as recited in Claim 17, wherein said
5 hash function includes a hash function $h': \{0, 1\}^* \rightarrow G \cup \{\perp\}$, that outputs
6 an element of G or \perp indicating a failure.

7
8 20. The computer-readable medium as recited in Claim 13, further
9 comprising:
10 outputting said digital signature.

11
12 21. The computer-readable medium as recited in Claim 20, further
13 comprising:
14 determining if said digital signature is valid using signature verifying logic.

15
16 22. The computer-readable medium as recited in Claim 21, wherein said
17 signature verifying logic is configured using said parameter data and said
18 parameter data establishes a base group G and a generator g as system parameters
19 for said signature verifying logic.

20
21 23. The computer-readable medium as recited in Claim 22, wherein:
22 said public key data includes public key data v ;
23 said identified data includes a message m ;
24 said digital signature includes signature σ ; and
25

1 determining if said digital signature is valid using said signature verifying
2 logic further includes:

3 determining $h \leftarrow h(m)$ using at least one hash function, and
4 verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple.
5

6 24. An apparatus comprising:

7 memory configured to store identifying data that is to be signed;

8 signature generating logic that encrypts data based on a Jacobian of a curve,
9 said Jacobian having a genus greater than one, said signature generating logic
10 being operatively coupled to said memory and configurable using parameter data,
11 said parameter data causing said signature generating logic to select at least one
12 Gap Diffie-Hellman (GDH) group of elements relating to said curve, and wherein
13 said signature generating logic determines private key data and corresponding
14 public key data, and then signs said identified data with said private key data to
15 create a corresponding digital signature.
16

17 25. The apparatus as recited in Claim 24, wherein said identified data
18 includes a message $m \in \{0, 1\}^*$.
19

20 26. The apparatus as recited in Claim 25, wherein said parameter data
21 establishes a base group G and a generator g as system parameters for said
22 signature generating logic.
23

24 27. The apparatus as recited in Claim 26, wherein said signature
25 generating logic determines said private key data and said public key data by:

1 picking $x \in \mathbb{Z}_p^*$; and
2 computing $v \leftarrow g^x$, wherein said public key data includes v and said private
3 key data includes x .

4
5 28. The apparatus as recited in Claim 27, wherein said signature
6 generating logic is further configured to:

7 determine $h \leftarrow h(m)$, and $\sigma \leftarrow h^x$, using at least one hash function, said private
8 key data x and said message m , wherein said digital signature includes σ .

9
10 29. The apparatus as recited in Claim 28, wherein said hash function
11 includes a full-domain hash function $h: \{0, 1\}^* \rightarrow G$.

12
13 30. The apparatus as recited in Claim 28, wherein said hash function
14 includes a hash function $h': \{0, 1\}^* \rightarrow G \cup \{\perp\}$, that outputs an element of
15 G or \perp indicating a failure.

16
17 31. The apparatus as recited in Claim 24, wherein said signature
18 generating logic is further configured to output said digital signature.

19
20 32. The apparatus as recited in Claim 31, further comprising:
21 signature verifying logic operatively coupled to receive said output digital
22 signature and determine if said digital signature is valid.

1 33. The apparatus as recited in Claim 32, wherein said signature
2 verifying logic is configured using said parameter data and said parameter data
3 establishes a base group G and a generator g as system parameters for said
4 signature verifying logic.

5
6 34. The apparatus as recited in Claim 33, wherein:
7 said public key data includes public key data v ;
8 said identified data includes a message m ;
9 said digital signature includes signature σ ; and
10 said signature verifying logic determines if said digital signature is valid by
11 determining $h \leftarrow h(m)$ using at least one hash function, and verifying that $(g,$
12 $v, h, \sigma)$ is a valid Gap Diffie-Hellman tuple.

13
14 35. The apparatus as recited in Claim 24, wherein said digital signature
15 is included in a product ID.

16
17 36. A method comprising:
18 receiving message data and a corresponding digital signature and public
19 key data;
20 using parameter data configure signature verifying logic that performs
21 cryptography operations based on a Jacobian of a curve, said Jacobian having a
22 genus greater than one, said parameter data causing said signature verifying logic
23 to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said
24 curve; and
25

1 with said signature verifying logic, determining if said digital signature is
2 valid using said public key data and said message data.

3
4 37. The method as recited in Claim 36, wherein said message data
5 includes a message $m \in \{0, 1\}^*$.

6
7 38. The method as recited in Claim 37, wherein said parameter data
8 establishes a base group G and a generator g as system parameters for said
9 signature verifying logic.

10
11 39. The method as recited in Claim 38, wherein:
12 said public key data includes public key data v ;
13 said digital signature includes signature σ ; and
14 determining if said digital signature is valid further includes:
15 determining $h \leftarrow h(m)$ using at least one hash function, and
16 verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple.

17
18 40. The method as recited in Claim 39, wherein said hash function
19 includes a full-domain hash function $h: \{0, 1\}^* \rightarrow G$.

20
21 41. The method as recited in Claim 39, wherein said hash function
22 includes a hash function $h': \{0, 1\}^* \rightarrow G \cup \{\perp\}$, that outputs an element of
23 G or \perp indicating a failure.

1 42. A computer-readable medium having computer implementable
2 instructions for causing at least one processing unit to perform acts comprising:
3 receiving message data and a corresponding digital signature and public
4 key data;
5 using parameter data configure signature verifying logic that performs
6 cryptography operations based on a Jacobian of a curve, said Jacobian having a
7 genus greater than one, said parameter data causing said signature verifying logic
8 to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said
9 curve; and
10 with said signature verifying logic, determining if said digital signature is
11 valid using said public key data and said message data.

12
13 43. The computer-readable medium as recited in Claim 42, wherein said
14 message data includes a message $m \in \{0, 1\}^*$.

15
16 44. The computer-readable medium as recited in Claim 43, wherein said
17 parameter data establishes a base group G and a generator g as system parameters
18 for said signature verifying logic.

19
20 45. The computer-readable medium as recited in Claim 44, wherein:
21 said public key data includes public key data v ;
22 said digital signature includes signature σ ; and
23 determining if said digital signature is valid further includes:
24 determining $h \leftarrow h(m)$ using at least one hash function, and
25 verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple.

1
2 46. The computer-readable medium as recited in Claim 45, wherein said
3 hash function includes a full-domain hash function $h: \{0, 1\}^* \rightarrow G$.

4
5 47. The computer-readable medium as recited in Claim 45, wherein said
6 hash function includes a hash function $h': \{0, 1\}^* \rightarrow G \cup \{\perp\}$, that outputs
7 an element of G or \perp indicating a failure.

8
9 48. A method comprising:
10 identifying data to be signed;
11 establishing parameter data for use with signature generating logic that
12 encrypts data based on a Weil pairing on a Jacobian of at least one super-singular
13 curve having a genus greater than one;
14 determining private key data and corresponding public key data using said
15 signature generating logic; and
16 signing said identified data with said private key data using said signature
17 generating logic to create a corresponding digital signature.

18
19 49. The method as recited in Claim 48, wherein said identified data
20 includes a message $m \in \{0, 1\}^*$.

21
22 50. The method as recited in Claim 49, wherein said signature
23 generating logic establishes E/F_p^l as an algebraic curve having genus g equal to at
24 least two, J being a corresponding Jacobian, such that $P, Q \in J$ are linearly
25 independent points of order q and $P \in J/F_{p^l}$ and $Q \in J/F_{p^a}$.

1
2 51. The method as recited in Claim 50, wherein determining said private
3 key data and said public key data includes:

4 picking $x \in Z_q^*$, and

5 computing $R \leftarrow xQ$, wherein said public key data includes R and said private
6 key data includes x .

7
8 52. The method as recited in Claim 51, wherein signing said identified
9 data using with said private key data using said signature generating logic further
10 includes:

11 determining $P_m \leftarrow h(m) \in J/F_{p'}$, and $S_m \leftarrow xP_m$, wherein said digital
12 signature includes σ , which is an x -coordinate of g points in a representation of S_m
13 as a reduced divisor.

14
15 53. The method as recited in Claim 48, further comprising:
16 outputting said digital signature.

17
18 54. The method as recited in Claim 53, further comprising:
19 determining if said digital signature is valid using signature verifying logic.

20
21 55. The method as recited in Claim 54, wherein said signature verifying
22 logic is configured to:

23 receive said public key as R , said identified data as a message m , and said
24 digital signature as σ ;

25

1 determine that said digital signature is valid for message m using said
2 public key data R , if $u = v$ after letting S be a point on J/F_p whose x -coordinates
3 is in σ and whose y -coordinate is y for some $y \in F_p$, and by setting $u \leftarrow e(P, S)$ and
4 $v \leftarrow e(R, \phi(h(m)))$;

5 otherwise determining that said digital signature σ is invalid.

6
7 56. The method as recited in Claim 48, wherein said digital signature is
8 included in a product ID.

9
10 57. A computer-readable medium having computer implementable
11 instructions for causing at least one processing unit to perform acts comprising:

12 identifying data to be signed;

13 establishing parameter data for use with signature generating logic that
14 encrypts data based on a Weil pairing on a Jacobian of at least one super-singular
15 curve having a genus greater than one;

16 determining private key data and corresponding public key data using said
17 signature generating logic; and

18 signing said identified data with said private key data using said signature
19 generating logic to create a corresponding digital signature.

20
21 58. The computer-readable medium as recited in Claim 57, wherein said
22 identified data includes a message $m \in \{0, 1\}^*$.

23
24 59. The computer-readable medium as recited in Claim 58, wherein said
25 signature generating logic establishes E/F_p^l as an algebraic curve having genus g

1 equal to at least two, J being a corresponding Jacobian, such that $P, Q \in J$ are
2 linearly independent points of order q and $P \in J/F_{p^j}$ and $Q \in J/F_{p^{ja}}$.

3
4 60. The computer-readable medium as recited in Claim 59, wherein
5 determining said private key data and said public key data includes:

6 picking $x \in Z_q^*$, and

7 computing $R \leftarrow xQ$, wherein said public key data includes R and said private
8 key data includes x .

9
10 61. The computer-readable medium as recited in Claim 60, wherein
11 signing said identified data using with said private key data using said signature
12 generating logic further includes:

13 determining $P_m \leftarrow h(m) \in J/F_{p^j}$, and $S_m \leftarrow xP_m$, wherein said digital
14 signature includes σ , which is an x -coordinate of g points in a representation of S_m
15 as a reduced divisor.

16
17 62. The computer-readable medium as recited in Claim 57, further
18 comprising:

19 outputting said digital signature.

20
21 63. The computer-readable medium as recited in Claim 62, further
22 comprising:

23 determining if said digital signature is valid using signature verifying logic.

1 64. The computer-readable medium as recited in Claim 63, wherein said
2 signature verifying logic is configured to:

3 receive said public key as R , said identified data as a message m , and said
4 digital signature as σ ;

5 determine that said digital signature is valid for message m using said
6 public key data R , if $u = v$ after letting S be a point on J/F_p whose x -coordinates
7 is in σ and whose y -coordinate is y for some $y \in F_p$, and by setting $u \leftarrow e(P, S)$ and
8 $v \leftarrow e(R, \phi(h(m)))$;

9 otherwise determining that said digital signature σ is invalid.

10
11 65. An apparatus comprising:

12 memory configured to store identifying data to be signed;

13 signature generating logic that is configured using parameter data such that
14 said signature generating logic encrypts data based on a Weil pairing on a
15 Jacobian of at least one super-singular curve having a genus greater than one, and
16 determines private key data and corresponding public key data and signs said
17 identified data with said private key data using said signature generating logic to
18 create a corresponding digital signature.

19
20 66. The apparatus as recited in Claim 65, wherein said identified data
21 includes a message $m \in \{0, 1\}^*$.

22
23 67. The apparatus as recited in Claim 66, wherein said signature
24 generating logic establishes E/F_p as an algebraic curve having genus g equal to at
25

1 least two, J being a corresponding Jacobian, such that $P, Q \in J$ are linearly
2 independent points of order q and $P \in J/F_{p^l}$ and $Q \in J/F_{p^{l\alpha}}$.

3
4 68. The apparatus as recited in Claim 67, wherein said signature
5 generating logic is further configured to:

6 pick $x \in Z_q^*$, and

7 determine $R \leftarrow xQ$, wherein said public key data includes R and said private
8 key data includes x .

9
10 69. The apparatus as recited in Claim 68, wherein said signature
11 generating logic is further configured to:

12 determine $P_m \leftarrow h(m) \in J/F_{p^l}$, and $S_m \leftarrow xP_m$, wherein said digital signature
13 includes σ , which is an x -coordinate of g points in a representation of S_m as a
14 reduced divisor.

15
16 70. The apparatus as recited in Claim 65, wherein said signature
17 generating logic is further configured to:

18 output said digital signature.

19
20 71. The apparatus as recited in Claim 70, further comprising:
21 signature verifying logic configured to receive said output digital signature
22 and determine if said digital signature is valid.

23
24 72. The apparatus as recited in Claim 71, wherein said signature
25 verifying logic is configured to:

1 receive said public key as R , said identified data as a message m , and said
2 digital signature as σ ;

3 determine that said digital signature is valid for message m using said
4 public key data R , if $u = v$ after letting S be a point on $J/F_{p'}$ whose x -coordinates
5 is in σ and whose y -coordinate is y for some $y \in F_{p'}$, and by setting $u \leftarrow e(P, S)$ and
6 $v \leftarrow e(R, \phi(h(m)))$;

7 otherwise determining that said digital signature σ is invalid.

8
9 73. The apparatus as recited in Claim 65, wherein said digital signature
10 is included in a product ID.